

~~CONFIDENTIAL~~

4 May 1986

MEMORANDUM FOR: Chief, Information Systems Security Division
Office of Security

25X1 FROM:

Chief, Management Division, M&CG
Office of Information Technology

SUBJECT: OIT Comments on PC Security Reference Guide (AIUO)

1. We distributed the PC Security Quick-Reference Guide to all groups within OIT for review. We have received many comments which are being included as an attachment to this memorandum. Item 2 of the Media Movement section, however, is of particular concern to this office. This item relaxes the current policy that under no conditions can undegaussed magnetic media used on a classified system (except tapes under special circumstances) be released to uncleared personnel. We believe that this policy should not be generally changed. Waivers to the policy, if necessary, should be granted on a case-by-case basis. To relax the policy generally could present a significant security risk.

2. Current Agency policy is at variance with item 2 under Media Movement. We would strongly recommend that this policy not be changed. In general, magnetic media should not be returned to vendors due to the possibility of contamination with classified information. This problem is greatly exacerbated by the large and growing number of relatively inexperienced PC users Agency-wide. Not only is it difficult to fully know the history of a specific diskette, it is also very difficult to properly examine the diskette for classified information. Routine users of PCs will not be able to reliably perform this task (even experienced users would have difficulty determining whether a specific diskette was fully and completely examined and no contamination was present.) We believe the procedures you have described in 1.g. of Media Labeling, as performed by a typical user, will not provide sufficient assurance that classified data have not been inadvertently written to the media.

3. Item 7 of the General Security Guidelines states that "Personally owned PC software or supplies, once used in Agency facilities, may not be removed." This policy should apply to any and all software used in Agency facilities unless a case-by-case waiver is supplied by your office. OIT is in the process of establishing a PC

~~CONFIDENTIAL~~

CONFIDENTIAL

Software Center for the purchase of PC software products on behalf of Agency employees. We plan to enter into licensing agreements with vendors which will stipulate that we will not return diskettes for any reason. In lieu of returning diskettes, we will destroy them in a secure manner and provide a memorandum to that effect for the vendor. While components may purchase software products on their own, they should be aware that a "no return" policy exists. Unless they establish this with a vendor at the time of the software purchase, the recommended "no return" policy may make them ineligible for updates or new releases of the product. Should problems arise with the "no return" policy, they should be handled on a case-by-case basis and treated as an exception to the rule. [redacted]

4. Agency policy concerning PC security must be straightforward and clearly presented to avoid confusion and overly loose interpretation of the rules. This office strongly opposes any statement encouraging the return of software to vendors under any conditions. [redacted]

5. For further information on the above comments or those in the attachment, please contact [redacted] of this office [redacted]. We appreciate the opportunity to comment on your draft guide. We believe the general concept of an easy-to-use reference document is a good one and encourage you, after careful consideration of our comments and others, to press ahead with publication. If I can be of any assistance, please let me know. [redacted]

Att: Further OIT Comments on PC Security Quick Reference Guide [redacted]

Distribution:

- addressee

CONFIDENTIAL

25X1

25X1

25X1

25X1

25X1

25X1

25X1

Page Denied

Next 2 Page(s) In Document Denied